WHAT IS CLAIMED IS:

pub A1

1. An apparatus for assessing a risk of a terrorist attack comprising:

a memory;

an input device;

a display device; and

a processor connected to the memory, the input device and the display device, the processor being configured to perform the steps of:

inputting information about a site of potential terrorist attack from a user;

constructing a model of the site based on the information input from the user;

accepting a designation from the user of a weapon and delivery point at the site;

determining an accessability of the site to the weapon/delivery point by determining a threat vector which is mostly likely the threat vector by which the weapon will be delivered and the likelihood of a successful delivery based on the model;

determining a probability that a terrorist attack will occur; and

calculating a relative risk based at least partially on the accessibility and probability.

2. The apparatus of Claim 1, wherein the relative risk is further based on a consequence calculation.

3. The apparatus of Claim 2, wherein the consequence calculations is performed by outputting data including model data to a consequence calculator plug-in and accepting consequence data from the plug-in.

pub A2

4. The apparatus of Claim 1, wherein the processor is further configured to perform the step of preparing a report including the ~~probability,~~ accessability and relative risk.

5. The apparatus of Claim 1, wherein the processor is further configured to perform the step of displaying a three dimensional representation of the most likely threat vector to the user.

Sub A3>

~~6. The apparatus of Claim 1, wherein the relative risk is calculated using a Bayesian network.~~

~~7. A method for assessing a risk of a terrorist attack comprising the steps of:~~

~~inputting information about a site of a potential terrorist attack from a user;~~

~~constructing a model of the site based on the input from the user;~~

~~accepting a designation from the user of a weapon and delivery point at the site;~~

~~determining an accessability of the site to the weapon/delivery point by determining a threat vector which is mostly likely the threat vector by which the weapon will be delivered and the likelihood of a successful delivery based on the model;~~

~~determining a probability that a terrorist attack will occur; and~~

~~calculating a relative risk based at least partially on the accessibility and probability.~~

8. The method of Claim 7, wherein the relative risk is further based on a consequence calculation.

9. The method of Claim 8, wherein the consequence calculations is performed by outputting data including model data to a consequence calculator plug-in and accepting consequence data from the plug-in.

Sub A4>

~~10. The method of Claim 7, wherein the processor is further configured to perform the step of preparing a report including the probability, accessability and relative risk.~~

11. The method of Claim 7, wherein the processor is further configured to perform the step of displaying a three dimensional representation of the most likely threat vector to the user.

Sub A5>

~~12. The method of Claim 7, wherein the relative risk is calculated using a Bayesian network.~~

~~13. A method of assessing risk comprising the steps of:~~

~~calculating a probability that an event will occur;~~

~~calculating a vulnerability to the event; and~~

calculating a relative risk based on the probability and vulnerability;

wherein the calculating steps are performed using an artificial intelligence network.

14. The method of Claim 13, wherein the artificial intelligence network is a Bayesian network.

15. The method of Claim 13, wherein the vulnerability is based upon a susceptability to the event and a consequence of the event.

16. The method of Claim 15, wherein the susceptability is based upon an accessability which is determined from a model of a physical environment.

17. The method of Claim 13, wherein the risk is a risk of a terrorist attack.

18. The method of Claim 13, wherein the risk is a risk of an infrastructure attack.

19. The method of Claim 13, wherein the risk is a risk of an information theft.

20. The method of Claim 13, wherein the risk is financial loss.

21. The method of Claim 13, wherein the risk is insurance loss.

22. The method of Claim 13, wherein the risk is environmental hazard.

23. The method of Claim 13, wherein the risk is risk of loss or damage to on-orbit satellite systems and constellations.

24. The method of Claim 13, wherein the risk is associated with air travel.

25. The method of Claim 13, wherein the risk is associated with highway travel.

26. The method of Claim 13, wherein the risk is associated with manned and unmanned space travel.

27. The method of Claim 13, wherein the risk is associated with military action.

28. The method of Claim 13, wherein the risk is injury to a person.

29. The method of Claim 13, wherein the risk is crime committed on a person.

30. The method of Claim 13, wherein the risk is a risk to home security.

31. The method of Claim 13, wherein the risk is a risk to building security.

32. The method of Claim 13, wherein the risk is program and project risk management.

33. An apparatus for assessing risk comprising:

a database for storing information including information about at least one actor, physical surroundings, and expert observations;

a simulation and gaming environment in communication with the database for determining a threat vector and a likelihood that the threat will succeed;

a plug-in interface in communication with the database and connectable to a consequence calculator for outputting information from the database to the consequence calculator and inputting information concerining a consequence of an undesirable event; and

a decision support system in communication with the database for calculating a relative risk based on probability and vulnerability determined from information in the database and information from the simulation and gaming environment and the plug-in interface.

34. The apparatus of claim 33, further comprising a report generator for assembling a report concerning the relative risk.

35. The apparatus of claim 34, further comprising a theater information management system for sharing database information with remote terminals or computers.

36. The apparatus of claim 33, wherein the database is an object oriented database.

37. The apparatus of claim 36, wherein objects in the database are persistent objects.

38. The apparatus of claim 33, wherein the information in the database further includes historical information.

39. The apparatus of claim 33, further comprising an editor for editing information in the database.

40. The apparatus of claim 33, wherein the risk is a risk of terrorist attack.

41. The apparatus of claim 33, wherein the decision support system employs a Bayesian network.